

January 26, 2004

THE USE OF COMMERCIAL OR EXTERNAL WEB HOSTING SERVICES FOR VHA WEBSITES

1. PURPOSE: This Veterans Health Administration (VHA) Directive establishes policy regarding VHA websites hosted by a commercial or external web hosting entity. ***NOTE:** The Directive also extends the applicability of existing information technology, web, data management, security, and privacy directives to websites that are hosted by a commercial entity or organization external to VHA. All applicable laws, regulations, and policies used to maintain system and data integrity within the Department of Veterans Affairs (VA) also apply to systems used on VA's behalf by VHA program offices, Veterans Integrated Service Network (VISN) offices, and contractors.*

2. BACKGROUND

a. Federal Government regulatory bodies, as well as VA and VHA, have created and issued a number of directives, acts, and provisions to account for the integrity of the data that VA collects, along with the security of the systems in which the data resides. These directives define the organizational responsibilities regarding the data posted on VHA Internet and Intranet websites.

b. The focus of the existing directives has been websites that are hosted within VA web hosting facilities or internal to a particular VA facility. However, the same security provisions must be applied to sensitive data hosted in commercial or external web servers as well.

3. POLICY: Effective management controls have been established and maintained Administration-wide for the creation and use of externally-hosted data to protect the integrity and security of sensitive data (such as patient data, employee data, and identifiable-quality assurance data); therefore, it is VHA policy that vendors who host sensitive data for any VHA entity must establish Business Associate Agreements, as defined under the Health Insurance Portability and Accountability Act, for the protection of individually-identifiable health information used or disclosed by business associates.

4. ACTION

a. **VISN Chief Information Officers (CIOs) and VA Central Office Program Officers.** The VISN CIOs and VA Central Office Program Officers are responsible for ensuring that commercial, or externally-hosted, VA websites must comply, no later than June 30, 2004, with the following:

(1) Externally-hosted VA Internet websites and related web services must be established, presented, managed, and maintained per VA Handbook 6102.

(2) Externally-hosted Systems of Records must be managed per the procedures published in VA Handbook 6300.5.

THIS VHA DIRECTIVE EXPIRES JANUARY 31, 2009

VHA Directive 2004-002
January 26, 2004

(3) External entities hosting VA data must comply with the process of Security Certification and Accreditation (C&A) of Information Systems as published in VA Directive 6214. **NOTE:** *An Interim Authority to Operate (IATO) must be obtained from VA's Office of Cyber Security while the C&A process is in progress.*

b. **Contracting Officers.** Contracting officers must place appropriate language in contracts informing vendors of the VA Internet, Intranet, and security guidelines to which vendors must adhere, per VA Directive 6214 and VA Directive 6210.

c. **Contracting Officer Technical Representative (COTR).** The COTR must ensure that an IATO is obtained and that the C&A process is completed according to VA Directive 6214.

d. **Organization's Web Manager.** The organization's Web manager must register the site in the VA Web Registry website and ensure that the contact information is current at all times (see <http://vaww.va.gov/webregistry>).

5. REFERENCES

- a. VA Directive and Handbook 6102, Internet and Intranet Services.
- b. VA Directive 6300, Records and Information Management.
- c. VA Handbook 6310.2, Collections of Information Procedures.
- d. VA Directive 6214, Information Technology Security Certification and Accreditation Program.
- e. VA Directive 6210, Automated Information Systems Security.
- f. VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act Systems of Records.

6. FOLLOW-UP RESPONSIBILITY: The Deputy CIO for Health (19), is responsible for the material contained in this Directive. Questions may be addressed to 202-273-8668.

7. RESCISSIONS: None. This VHA Directive expires January 31, 2009.

Nevin M. Weaver for
Robert H. Roswell, M.D.
Under Secretary for Health

DISTRIBUTION: CO: E-mailed 1/29/04
FLD: VISN, MA, DO, OC, OCRO, and 200 – E-mailed 1/29/04